State of Maine

Department of Administrative & Financial Services

Office of Information Technology

Security Assessment and Authorization Policy and Procedures (CA-1)

Table of Contents

1.0 Document Purpose:

The purpose of this document is to define the State of Maine policy and procedures about how the Office of Information Technology (OIT) conducts and supports security assessments (e.g., host, system, network, procedure, personnel, etc.) to determine if it is successful in meeting specific security objectives.

2.0 Scope:

2.1 This policy applies to all State of Maine employees and contractors (collectively referred to as personnel in this document) with access to:

2.1.1 Executive Branch Agency information assets, irrespective of location; and

2.1.2 Information assets from other State government branches that use the State network.

3.0 Policy Conflict:

If this policy conflicts with any law or union contract in effect, the terms of the existing law or contract prevail.

4.0 Roles and Responsibilities:

4.1 **Agencies are responsible for:**

4.1.1 Ensuring that any contracts for vendor-hosted/managed agency information systems adhere to any pertinent federal regulations, state regulations, and Office of Information Technology (OIT) policies, procedures, and standards.

4.1.2 Ensuring agency personnel are aware of all applicable penalties for non-compliance.

4.1.3 Developing and implementing agency-level policy and procedures, to meet any additional, pertinent security assessment and authorization regulatory compliance requirements.

4.1.4 Directly coordinate to meet all state and federal audit documentation, reporting, and on-site logistic support compliance requirements.

4.2 **Office of Information Technology (OIT):**

4.2.1 **IT Vendor Management is responsible for:**

4.2.1.1 Ensuring interconnections with vendors are properly documented.

4.2.1.2 Ensuring vendor contracts contain appropriate security requirement language.

4.2.2 **Information Security Office (Infrastructure) is responsible for:**

4.2.2.1 Conducting assessments to identify information technology system's exploitable weaknesses.

4.2.2.2 Using assessment results to increase OIT's ability to maintain a proactive information security defense.

4.2.3 **Information Security Office (Governance) is responsible for:**

4.2.3.1 Remediating known, systemic information security audit findings, and developing systems to improve State of Maine information security inspection results.

4.2.3.2 Assisting State of Maine agencies to improve the security for numerous data types to include, but not limited to, Federal Tax, Social Security, Affordable Care Act, Criminal Justice, Credit Card, Health and Personally Identifiable Information.

4.2.3.3 Providing information technology responses and assist with finding remediation to security audits conducted by the Internal Revenue Service (IRS), Centers for Medicare and Medicaid Services (CMS), Federal Bureau of Investigation (FBI), U.S. Department of Health and Human Services (US DHHS), Social Security Administration (SSA), private security companies, and State of Maine agencies.

5.0 Management Commitment:

The State of Maine is committed to following this policy and the procedures that support it.

6.0 Coordination Among Agency Entities:

The Office of Information Technology (OIT) works with agencies to meet all state and federal compliance requirements related to information security. OIT cooperatively assesses the security controls of information systems and its environment of operation as outlined in this document to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements.

7.0 Compliance:

7.1 For State of Maine employees, failure to comply with the procedures identified in this policy may result in progressive discipline, up to and including dismissal.

7.2 For State of Maine contractors and non-State of Maine personnel, failure to comply may result in removal of the individual's ability to access and use State of Maine data and systems. Employers of non-State of Maine personnel will be notified of any violations.

7.3 Personnel are also subject to any applicable penalties for statutory requirements compliance violations. Depending on the requirement and the nature of the violation, penalties could include fines and/or criminal charges.

8.0 Procedures:

8.1 The following represent the security controls established to meet an acceptable level of protection for State of Maine information systems. They serve as the base set of procedural requirements that are implemented to provide security assessment and authorization. For the components and products that they are responsible for, the Office of Information Technology does the following:

8.2 **Security Assessment (CA-2 including CE-1):**

8.2.1 Information Security Office (Governance) works with agencies and the other business units of OIT to facilitate the completion of federal and state audits, remediate audit findings, and assist with the completion of associated documentation.

8.2.2 The planned on-site security control assessments and assessment report requirements that meet federal statutory requirements are found in Appendix A – Security Assessments. The onsite audits listed in this appendix are conducted by independent, third-party assessors.

8.2.3 In addition to the audits and reports found in Appendix A, ad-hoc security control assessments and assessment reports are determined by the Chief Information Security Officer (CISO), Chief Information Officer, and other State of Maine agencies. These assessments are typically conducted through contracts with professional service firms to conduct security audits and selected based on their ability to conduct impartial assessments of the organization. The scope of these assessments is based on needs at the time the firm is engaged. Professional service firm audits that involve OIT support must be approved by the CISO prior to contract approval.

8.2.4 Security assessments are also conducted by:

8.2.4.1 The State of Maine conducts both ad hoc (e.g., Office of Program Evaluation and Government Accountability) and routine (primarily through the Office of the State Auditor) security inspections as authorized by statute. The scope of these assessments varies but does provide OIT with findings related to security.

8.2.4.2 Information Security Office (Infrastructure) and Network Security (Perimeter) primarily conduct continuous monitoring and works with the other business units for remediation of findings.

8.2.4.3 Every 18 months, Information Security (governance) coordinates with the State of Maine agencies that handle Federal Tax Information (FTI) for the completion of internal inspection of all OIT locations that contain FTI (excluding Federal Risk and Authorization Management Program certified sites) to include:

8.2.4.3.1 Iron Mountain Inc., Scarborough, Maine

8.2.4.3.2 Sewall Street Data Center

8.2.4.3.3 Commerce Street Data Center

8.2.4.4 System development life-cycle activities assess risk as a part of both the deployment certification and change management processes (described more in 8.5.2 below)

8.3 ***System Interconnections*** **(CA-3 including CE-5):**

8.3.1 OIT has documented system interconnections with vendors using Service Level Agreements (SLAs), Memorandums of Agreement (MOAs) and contracts.

8.3.2 Interconnection documentation must document:

8.3.2.1 The technical and security requirements for establishing, operating and maintaining the interconnection; and

8.3.2.2 The terms and conditions for sharing data to include:

8.3.2.2.1 The purpose of the interconnection;

8.3.2.2.2 Identifying the relevant authorities

8.3.2.2.3 Specifying the responsibilities of both organizations

8.3.2.2.4 Defining the terms of agreement including

8.3.2.2.4.1 Apportionment of costs; and

8.3.2.2.4.2 The timeline for terminating or reauthorizing the interconnection.

8.3.3 OIT-managed firewalls universally enforce a deny-all-allow-by-exception rule for all external traffic seeking entry into the state network. Also, all access is universally secured by authentication credentials, encrypted both at rest, and in motion. See Access Control Policy and Procedures (AC-1)[1] for more information.

8.4 **Plan of Action and Milestones (POA&M) (CA-5 including CE-1):**

8.4.1 The OIT process for POA&M development and review is as follows:

8.4.1.1 Information Security Office (Governance) maintains a consolidated POA&M. The consolidated POA&M is based on:

8.4.1.1.1 Audit results;

8.4.1.1.2 Gaps in policy and procedures; and

8.4.1.1.3 POA&M findings for certain federal audits (e.g., IRS, CMS, SSA) for findings that OIT is responsible for.

8.4.1.2 OIT reviews the consolidated POA&M with the Chief information Security Officer quarterly in the months of September, December, March, and June.

8.4.1.3 The POA&M includes any necessary corrective actions identified during the internal inspection outlined in Security Assessments (CA-2) (coming soon) and identifies the actions OIT plans to take to resolve these findings. See Plan of Action and Milestones (CA-5) (coming soon) for more information.

8.4.1.4 Information Security Office (Governance) employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.

8.4.2 Agencies may have to establish and maintain a POA&M for agency level findings to meet regulatory compliance requirements.

8.5 **Security Authorization (CA-6):**

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/access-control-policy.pdf

8.5.1 The Chief Information Officer (CIO) is the senior-level executive, head of OIT, who serves as the authorizing official for applications and computer infrastructure for State of Maine agencies.

8.5.2 OIT partners with supported agencies to make the final determination whether applications and computer infrastructure are placed into production based on the following OIT policies:

8.5.2.1 OIT Infrastructure Deployment Certification Policy[2]

8.5.2.2 OIT Application Deployment Certification Policy[3]

8.5.2.3 OIT Change Management Policy[4]

8.5.3 OIT change management procedures address, among other processes, system quality assurance development and testing change management. These documents outline the authorities and roles involved in the process of a significant change to State of Maine infrastructure.

8.5.4 Agencies should develop and implement their own internal Change Management procedures.

8.5.5 See OIT System and Services Acquisition Policy and Procedures (SA-1) (coming soon) for additional authorization requirements for information system changes that occur as a result of the acquisition process.

8.6 Continuous Monitoring (CA-7 including CE-1):

8.6.1 OIT monitors all its information assets to detect attacks, and indicators of potential attacks, as well as unauthorized local, network, and remote connections.

8.6.2 OIT performs continuous monitoring of information systems, including:

8.6.2.1 Real-time scans at network entry and exit points to detect and eradicate malicious code

8.6.2.2 Weekly scans of information systems and real-time scans of files from external sources

[2] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/infrastructure-deployment-certification.pdf

[3] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/application-deployment-certification_0.pdf

[4] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/change-management-policy.pdf

8.6.2.3 Ongoing security control assessments

8.6.2.4 The Information Security Office generates internal security alerts, advisories, and directives as deemed necessary (e.g., in response to a known issue, a known threat, or to strengthen the state's security posture).

8.6.3 OIT generates a monthly report which identifies the amount of SPAM received, by type (phishing, viruses, or non-repudiation).

8.6.4 Response actions are managed through a plan of actions and milestones (POA&M). See section 8.4.

8.7 **Internal System Connections (CA-9):**

8.7.1 State of Maine employees and contractors are prohibited from connecting any new devices to any State of Maine network for any reason. For additional information, see the Network Device Management Policy[5].

9.0 Document History and Distribution:

Version	Revision Log	Date
Version 1.0	*Initial Document*	*September 6, 2019*

Approved by: Chief Information Officer, OIT.

Legal Citation: Title 5, Chapter 163: Office of Information Technology[6].

Distribution

This document will be distributed to all appropriate State of Maine personnel and will be posted on the OIT website (https://www.maine.gov/oit/policies-standards).

10.0 Document Review:

This document is to be reviewed annually and when substantive changes are made to policies, procedures or other authoritative regulations affecting this document.

11.0 Records Management:

Office of Information Technology security policies, plans, and procedures fall under the *Routine Administrative Policies and Procedures and Internal Control Policies and*

[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/network-device-management-policy.pdf

[6] http://legislature.maine.gov/statutes/5/title5ch163sec0.html

Directives records management categories. They will be retained for three (3) years and then destroyed in accordance with guidance provided by Maine State Archives. Retention of these documents will be subject to any future State Archives General Schedule revisions that cover these categories.

12.0 Public Records Exceptions:

Under the Maine Freedom of Access Act, certain public records exceptions may limit disclosure of agency records related to information technology infrastructure and systems, as well as security plans, procedures or risk assessments. Information contained in these records may be disclosed to the Legislature or, in the case of a political or administrative subdivision, to municipal officials or board members under conditions that protect the information from further disclosure. Any aggrieved person seeking relief for an alleged violation of the FOAA may bring suit in any Superior Court in the state.

13.0 Definitions:

13.1 **System Interconnection:** The direct connection of two or more IT systems for the purpose of sharing data and other information resources.

13.2 **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Appendix A – Federal Security Assessments

1.0 Internal Revenue Services (IRS) Related Items

1.1. Reference: IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies.

1.2. IRS Office of Safeguards On-Site Review – Every three years, the IRS assesses all security controls and enhancements during an on-site review of all agencies that receive, process, or store Federal Tax Information (FTI). The team from IRS Office of Safeguards uses both testing, and interviewing assessment methods. The IRS issues a Safeguard Review Report (SRR) and a Corrective Action Plan (CAP) to document its on-site review findings.

1.3. Safeguard Security Report (SSR) Development – The SSR is the document where the agencies that receive FTI (Maine Revenue Services (MRS), Department of Labor (DOL), and the Department of Health and human Services (DHHS)) provide the IRS with a self-assessment describing the current state of security. Agencies that receive FTI submit a yearly update (due May 30) of the SSR which is accompanied by a certification of accuracy signed by the appropriate Director. The SSR addresses all security controls and enhancements using interviewing assessment methods.

1.4. CAP Development – agencies that receive FTI submit their updated CAP semi-annually: (i) as an attachment to the SSR on May 30; and (ii) separately on the CAP due date, November 30. The CAP assesses all security control deficiencies identified during the IRS on-site audit. For outstanding findings, agencies that receive FTI list actions taken, or planned, to implement recommendations from the SRR issued because of an IRS on-site review. Supporting documentation is required to close any finding identified as a critical or significant risk to FTI. The IRS tracks all review findings in a database until the findings are closed with an implementation date via the CAP update process. OIT is responsible for corrective action plans and remediation of all select findings (i.e., tab H) and any physical findings on OIT locations or data centers.

1.5. Internal Inspection

1.5.1. The IRS requires internal inspections by the agencies that receive, process, or store Federal Tax Information (FTI). The purpose is to ensure that the security policies and procedures established by the agency to protect FTI are functioning, maintained and enforced. The inspection of OIT facilities is conducted every 18 months. Even though this internal inspection is focused on the security of FTI, it provides OIT an objective assessment of information security for all OIT facilities and has applicability beyond FTI.

1.5.2. The IRS also requires inspection of vendors that handle FTI for an agency that are not already FEDRAMP certified. Iron Mountain stores backup tapes of our data, including FTI data. External inspections are done to ensure that the security policies and procedures established by the vendor to protect FTI are functioning, maintained and enforced. External inspections are conducted every 18 months. Only one of the agencies using a vendor is required to conduct the inspection and provide the inspection report to the other agencies.

2.0 Social Security Administration (SSA)

2.1. Reference: Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with The Social Security Administration.

2.2. Social Security Administration (SSA) On-Site Compliance Review - Every three years, the SSA assesses all security controls and enhancements during an on-site review of all agencies that receive, process, or store SSA Information. The team from the SSA uses both testing and interviewing assessment methods. The SSA issues a formal report to document its on-site review findings. Updates to these findings are due to the SSA quarterly until resolved.

2.3. Compliance Review Questionnaire (CRQ) – agencies that receive information from the SSA, submit an updated CRQ triennially prior to the On-Site Compliance Review. The CRQ describes the agencies management, operational, and technical controls used to protect SSA-provided information from misuse and improper disclosure.

3.0 Federal Bureau of Investigation (FBI)

3.1. Reference: CJISD-ITS-DOC-08140-5.7, Criminal Justice Information Services (CJIS) Security Policy.

3.2. CJIS On-Site Security Inspection - At a minimum, the CJIS audit manager triennially audits all agencies and contractors with access to federally provided Criminal Justice Information. The FBI uses direct access to the state system to ensure compliance with applicable statutes, regulations and policies.

3.3. CJIS Pre-Audit Questionnaire – A few months before the CJIS audit is conducted, the State of Maine receives a pre-audit questionnaire. The pre-audit questionnaire is used to assist the audit manager in gathering pertinent information prior to the on-site visit. Information gathered from the pre-audit questionnaire is used to formulate additional questions to be answered during the on-site visit and to assist in determining policy compliance.

4.0 Center for Medicare and Medicaid Services (CMS)

4.1. Reference: MARS-E Document Suite, Version 2.0 Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges.

4.2. MARS-E 2.0 Security Controls Assessment (SCA) - At a minimum, CMS requires an on-site SCA triennially be conducted by CMS, or an approved third party, for all agencies with access to federally provided Affordable Care Act Data (ACA). The SCA includes the examination of documents, settings, configurations, controls, and interviews of organizational personnel and technical testing. The purpose of an SCA is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the information system.

4.3. Security and Privacy Controls Assessment Test Plan - The Security and Privacy Controls Assessment Test Plan documents all testing to be conducted during the assessment to validate the security and privacy controls for agencies with access to ACA data.

4.4. ACA Administering Entity System Security Plan (SSP)- The SSP documents the compliance with mandates of the ACA legislation and Department of Health and Human Services (HHS) Regulations for agencies that receive ACA data. The System Security Plan is the key tool for describing the IT security and privacy environment for IT systems and for documenting the implementation of security and privacy controls for the protection of all data received, stored, processed, and transmitted by the ACA IT systems and supporting applications. The SSP must be initiated during the initial stages of the life cycle process for IT systems and maintained thereafter.

4.5. Security Assessment Report (SAR) - At the completion of the SCA, the assessor provides a SAR. The SAR presents the findings of the assessment annotated in detail with the remediation recommendations for the weaknesses or deficiencies found in the information system security controls implementation. Findings in the SAR must be reported and monitored until remediation in a Plan of Action and Milestones.

5.0 U.S. Department of Health and Human Service (U.S. DHHS), Office for Civil Rights (OCR)

5.1. References:

5.1.1. U.S. DHHS Audit Protocol, July 2018;

5.1.2. HIPPA Security Series, Volume 2, Paper 1 through 7; and

5.1.3. HIPAA Privacy, Security, and Breach Notification Audit Program, hhs.gov

5.2. Desk Audits - OCR expects covered entities that are the subject of an audit to submit requested information via OCR's secure portal within 10 business days of the date on the information request. After these documents are received, the auditor will review the information submitted and provide the auditee with draft findings. Auditees will have 10 business days to review and return written comments, if any, to the auditor. The auditor will complete a final audit report for each entity within 30 business days after the auditee's response. OCR will share a copy of the final report with the audited entity.

5.3. On Site Audits - Similarly, entities will be notified via email of their selection for an onsite audit. The auditors will schedule an entrance conference and provide more information about the onsite audit process and expectations for the audit. Each onsite audit will be conducted over three to five days onsite, depending on the size of the entity. Onsite audits will be more comprehensive than desk audits and cover a wider range of requirements from the HIPAA Rules. Like the desk audit, entities will have 10 business days to review the draft findings and provide written comments to the auditor. The auditor will complete a final audit report for each entity within 30 business days after the auditee's response. OCR will share a copy of the final report with the audited entity.